ئەم کاتەتان باش هاوڕێیان

پێشەکی

سوپاسی خودای گەورە دەکەم کە ئەم دەرفەتەی پێدام بۆ بەخشینی کەمێك لەو ڕاتانەی کە کۆم کردوونەتەوە و پێشکەشی ئێوەی دەکەم ئینشاالله.

کورتەیەك دەربارەی ڕاتەکان RATs

ڕات چی یە؟

بەرنامەیەك Software ێکە هەر وەك پۆلی بەرنامە ئاساییەکانی دیکە ، بەڵام بەکار و پیشەی جودا ، هەڵدەستێت بە دەستبەسەراگرتن Remote کردنی وەگەڕخەر Operator ـێك.

شێوازی کارکردنی ڕاتەکان فیزیکاڵە Physical Access ـە ، واتە شێوازێکی خودکارانەی هەیە و دەتوانێت بڵاوببێتەوە بەسەر سیستەمدا و جێگیر ببێت لەسەر فایلێك بەنموونە ، هەر ئەم تایبەتمەندیەی وایکردووە کە زۆرجار فایلەکانی دیوی سێرڤەر -Server Files- پێی بگوترێت -Trojan- ترۆجـان.

ترۆجان چی یە؟

ئەگەر بەشێوەیەکی درووست لە ڕاتەکان بڕوانین ، دوو میتۆد بەڕێوەی دەبات:

1. فایلی هاوپێچ و درووستکراوی (Client).
2. فایلی هاوپێچ و درووستکراوی (Server).

بەڵام کاتێك هەردوك فایل بەهۆی بەرنامەیەکی وەکو ڕات -RAT- دەبەسترێت بەیەکەوە ئەوکات دەتوانین پێی بڵێین -Trojan- کەواتە فایلی هاوپێچی دیوی (Client + Server) پێکەوە ترۆجانێك درووست ئەکەن کە بەهۆی ڕێڕەوێکەوە -DNS- داتا ئاڵوگۆڕ دەکات ، وەهەرکات Domain Name System پێشکێش بە فایلەکە کرا ئەوکات ترۆجان دەبێتە (Trojan Horse) واتە (ئەسپی ترۆین) ، لێرەدا ئەسپەکە دۆمەینە وەك No-IP کە یاریدەی جێگیرکردنی ئایپی دەدات بەهۆی دامەزراوەیەکی سیستەم لەسەر هۆستێك یاخود ئایپیەك. بەکورتی فایلە هاوپێچکراوە دوانییەکە ترۆجانە و هۆستەکەش لەسەر دۆمەینێك (DNS) ئەسپە گەیەنەرەکەیە.

لێرەدا پرسیارێك درووست دەبێت: ئایا ڕاتەکان تەنها بۆ مەبەستی هاك کردن بەکار دێت؟

نەخێر ، ڕاتەکان لەبنەڕەتدا بەرنامەی هاك نین تا هاکەر هاکی پێ بکات ، بەڵکو تەنها بەرنامەی فێرکارین لەبۆ فێرگەکان. بەڵکو بەهۆی ڕاتەکانەوە گەشەپێدەر نەك هاکەر ، ترۆجانێك هاوپێچ دەکات و بەکاری دێنێت بۆ دەستبەسەرا گرتن.



شێوازی کەللەسەری سەربازێکی جەنگی تەروادە (یۆنان)

لە بواری هاکیشدا یـۆنان -گریك-

مێژووی ترۆجان ، جەنگی تەروادەمان بیر دەخاتەوە کاتێك بۆ تۆڵەسەندنەوە هیکتۆری پادشا ، چوو تۆڵە بستێنێتەوە لەبری ئامۆزا کوژراوەکەی لە یۆنان ، بەڵام سەربازی کەم بوو ، ناچار پلانێکی دارشت بۆ ئەوەی زەبرێکی توند بدات لەدوژمن ، هەربۆیە تـــرۆجـانی درووست کرد ، ئەم ڕووداوە گرنگە بۆ هاککەران.

دواتر هیکتۆر هات ئەسپێکی درووستکرد بە تەختە و پڕی کرد لە سەرباز و بەدیاری ناردی بۆ پادشای دوژمن ئەم ئەسپە ئەوەندە زەبەلاح بوو هەموو خەڵکی شار سڵیان دەکردەوە ، لەشەودا بوو ئەسپەکە بە پاڵ پێوەنان بەهۆی ڕەورەوە -تایە- کانیەوە تابەیانی دواتر برا بۆ ناو شاری دوژمن ، و کرا بەدیاری ، بەڵام لەنیوەشەودا سەربازانی ناو ئەسپەکە بەجارێك خۆیان هاویشتە دەرەوە و دایان بەسەر شاردا و تەفرو تونایان کرد.

بەم شێوەیە بەهۆی ترۆجانێکەوە (فایلێکی هاوپێچ) دەستگیرا بەسەر وەگەڕخەری شار (سیستەم)ی دوژمن.



وێنەی کێشراوی ئەسپی تەروادە (Trojan Horse)

ڕوونکردنەوەی وێنەکە:

خەڵکەکە: (Victim-کەسی قوربانی)

تایەکان: (Link-لینك)

سەربازەکانی ناوی: (ڤایرۆسەکان)

نامەکەی هێکتۆر و کرێکارەکان: (دەمج binder)

شارەکە: (سیستەم system)

پەت (گوریسەکان): (Mose Click-کیلك)

سیاستی هیکتۆر: (Aim-ئامانج-RAT)

سیستەمی دوژمن

Remote Access Tool :RAT ، خەڵك دوو جۆر بەکاری دێنێت:

1. ترۆجانێك درووست دەکات و دەیکاتە شاری دوژمن ، یاخود سیستەمی دوژمن (ئەگەر دوژمنت هەیە ئەوە بکە بۆی).
2. دوو فایلی هاوپێچی درووستکراو ، سێرڤەر و کلاینت ، بۆ مەبەستی فێرکاری لە دام و دەزگا حکومیەکان و قوتابخانەکانی ئایتی دا.

ئیشی ڕاتەکان بەگشتی

دەتوانین ئیشی ڕاتەکان دابەش بکەیت بەسێ لقەوە:

أ. ڕاتی مەبەست دار: مەبەست لەم جۆرە ڕاتە ئەوەیە کە گەشەپێدەر (Developer) بۆخۆی بەزمانێك ڕاتێك درووست دەکات کە تەنها مەبەست لێی یەك جۆر ئیشە بۆ سەر کارپێکراوی قوربانی (Access Victim) و دەیەوێت تەنها یەك کار بکات ، بەزۆری سیخوڕەکانی بواری پاراستن ئەم جۆرە لەڕات درووست دەکەن تەنها بۆ یەك مەبەست.

ب. ڕاتی بێ مەبەست: بریتیە لەو دوو فایلە پەستێنراوە هاوپێچیەی کە بۆ هیچ مەبەستێکی دەست بەسەرا گراتن بەکار نایەت ، چونکە ئەگەر مەبەستداربێت کەواتە کەسانی هاکەر بەکاری دەبەن ، وە ئەم جۆرە تەنها لەتۆڕی ناوخۆیی دا کاری پێ دەکرێت ، وەك فێرگەکان.

ج. ڕاتی گشت: ترسێنەرە و هاکەر بەکاری دەبات و دەیکات بەترۆجان ، کە بەڕاتی (RAT through a network connection) ناسراون ،ئەمەیان قسە زۆر هەڵدەگرێت بەڵام بەگشتی ئیشەکانی دەکەین بە چەند بەشێکەوە:

1. دەست دەگرێت بەسەر کامێرادا.
2. داتاکان ئاڵوگۆڕ دەکات.
3. شێڵ کردن (ئیشی CMD).
4. ئیشەکانی هاردوێر (پارچە ڕەقەکان) دەکات.
5. ڕیجستەری (داتا شاراوەکانی سیستەم)
6. هێرش کردن (Attack)
7. دامەزراندنی نەرمەکاڵا (Software)
8. ڕیموت کردنی دیسکتۆپ.
9. تاسك مانجەر بۆ داخستن و کردنەوە.
10. ..هتد.

ڕاتەکان پێویستیان بە چی هەیە؟

بۆ ئەوەی بەباشی ڕاتێك بەتایبەتی جۆرە گشتیەکەی ، جێگیر بکەیت لەسەر سیستەمەکەت پێویستە ڕەچاوی ئەم خاڵانە وەك یاسا بکەیت هەتاوەکو بەباشی ڕاتێکی نموونەیی گشتی بەکاربهێنیت و ئیش بکـات بەبێ کێشە. خاڵەکان یاخود یاساکان:

1. لەڕووی سایکۆلۆژیەوە (دەروونی)

کەسێتی تۆ پێویستە پێش ئەوەی ڕاتێك بەکاربهێنیت ، دەروونی خۆت بناسیت ، تا ئەگەر بێت و کەسێتی شێلگیر و تورە بیت پێم وایە خراپە ڕات بەکاربهێنیت ، چونکە دواجار بەزەرە و زیانی خۆتدا دەشکێتەوە و ئەوەندەی تر باری دەروونیت لاواز دەبێت ، بۆیە کەسێتی خۆت زۆر گرنگە.

2. ئامانج

فێربوونی ڕاتەکان بۆ ئامانجە ، هەتا ئامانجێکت نەبێت وا باشترە خۆت فێر نەکەیت ، خۆ ئەگەر بەبێ ئامانج ڕات بەکاربهێنیت ئەوا باشترە ، چونکە بۆ پۆلی دوومیت لە جۆری ڕاتەکان (تەنها خۆت فێر دەکەیت).

3. ڕاتێك دەستنیشان بکە

زۆر بگەڕێ هەتا ڕاتێك دەدۆزیتەوە کە زۆر سەرنجت ڕادەکێشێت ، بڕۆ پرسیار لەکەسانی بەئەزموون بکە ، خۆت بگەڕێ ، دواجار ڕاتێك دەستنیشان بکە و بیکە بە هاوڕێت بەڵێ (My RAT Friend for Ever) من هاوڕێیەکم هەیە زۆرم خۆش دەوێت و زۆریش نهێنیە ، لە کۆمپیوتەرەکەمدایە ، هەرکات کە دەیکەمەوە ئارامی بە دڵمدا دێت ، ئەگەرچی ئەو هاوڕێیەشم هیچم پێشکەش ناکات.

4. ڕات چی یە؟

نەك ڕات RAT , بەڵکو ڕات چی یە دەربارەی هاوڕێکەت RAT؟ ئەم پرسیارە وەك ئەوە وایە بڵێی: من کێم؟ دەی کەواتە بگەڕێ بزانە ڕات چی یە بەرامبەر بە RAT؟

5. دەرگاکەی لێ بکەرەوە

Port دەرگە و دەرچەیە ، پۆرت بکەرەوە ، هەرچۆنێك بێت تۆ دەبێت نان بدەیت بەهاوڕێکەت تا ئەویش سودت پێ بگەیەنێت.

6. DNS دابمەزرێنە

ناکرێت و ناشێت هەرچی ئیشێك کە هاوڕێکەم RAT بۆم دەکات بچێت بۆ تۆ! ، کەوایە ڕاتکەت توندوتۆڵ بکە و ئایپیەکەت جێگیری بکە بەهۆی دۆمەینێکەوە با ئەو ئیشەی ڕاتەکە دەیکات بێتەوە بۆ ئەمرەکەی تۆ.

7. تاقیکردنەوە باشترین بەڵگەیە

سیستەمێکی تاقیکاری (تاقیگە) دابمەزرێنە بە خەیاڵی (Virtual System) بۆ تاقیکردنەوەی کارەکانت.

8. وریابە (ئاگاداربە) (Warning)

هەندێك جار ڕاتەکانیش بێ وەفان ، بگەڕێ و لەکۆتایدا ئەمەت بۆ دەردەکەوێت.

9. ئێستاش خاڵی یەکەم سەیر بکەرەوە؟!

(من ڕاتە گشتیەکان بەکار ناهێنم چونکە زۆر کەسێکی هەڵچوم)

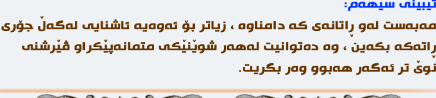
وەرە ڕاتێك بکە بەهاوڕێت

لەجیهاندا زۆر ڕاتی گشتی (Public) هەن کە توانایا بێ سنوورە لەدەست بەسەرا گرتن ، وە تۆ تاکو ئێستاش هاوڕێیەکی بەنرخت نیە ، چونکە گومانت هەیە ، ئەوەتا لێرە کۆمەڵێك ڕاتی جیاواز دەبینیت ، وە لەوانەیە تۆش بێ وەفا دەربچیت بەرامبەر بەڕاتە کۆنەکەت.

بەهەرحاڵ زۆرێك گەڕاوم و زۆر ماندو بووم تاکو توانیم ئەم ڕاتانە کۆبکەمەوە و لە بابەتێکدا بۆ ئێوەی خۆشەویستی دابنێم .

تێبینی:

زۆربەی ئەوڕاتانەی لەبەشی (ڕاتەکان - RAT) هەیە دام نەناون ، تۆ دەتوانیت لەوێ هاوڕێیەك دەستنیشان بکەیت.



تێبینی دووەم:

لەسەرەوە ناو وە وێنە و ژمارەی ڕاتەکان دادەنێم ، چونکە فێرکاریەکە وێنەییە ، و لەخوار وێنەی RATەکانەوە ئەگەر ڕاتێکت بەدڵ بوو دەتوانی بەژماری وێنەکەیدا لەخوارەوە دایبگریت.

تێبینی سێهەم:

مەبەست لەو ڕاتانەی کە دامناوە ، زیاتر بۆ ئەوەیە ئاشنایی لەگەڵ جۆری ڕاتەکە بکەین ، وە دەتوانیت لەهەر شوێنێکی متمانەپێکراو ڤێرشنی نوێ تر ئەگەر هەبوو وەر بگریت.

لە کـۆتایی دا

سوپاس و ستایشی خودای گەورە دەکەم کە هانی دام بۆ تەواو کردنی بابەتەکە و سوپاسی بەڕێوەبەری ئەم یانەیە (هەنگاو هەولێری) دەکەم کە کەمەك یارمەتی دام ، و سوپاسی ئەندامان و سەرپەرشتیاران دەکەم.

چەند شتێك هەیە پێویستە لە بەشی کۆتایی دا بیڵێم , دەمەوێت سەبارەت بە کورتکراوەی RAT ئاماژە بدەم , زۆرێك لە شوێنە گرنگ و بەئەزموونەکان درێژکراوەی RAT بە چەند شێوەیەك دێتە ناو جیهانی چەمکەکانی کۆمپیوتەرەوە , جا بەکارهێنەر دەتوانێت چەمکێك بکاتە سەر بنەڕەتی کورتکراوەکە , لەوانە:

- بەهۆی ئەوەی لەبواری هاکدا زۆرێك لە بەکاربەرانی ڕات بۆ مەبەستی دەستبەسەرا گرتن و بەڕێوەبردن بەکاری دەهێنن کەواتە لێرەدا RAT کورتکراوەکەی بەم شێوەیەیە (Remote Administration Tool) یاخود لەبەر ئەوەی تەنها یەك تووڵ نیە ئەوا (Remote Administration Tools).
- سەبارەت بەجۆر و شێوەی بەکارهێنانی ڕاتەکان ڕێڕەو و بۆچونێکی دیکەش هەیە لەسەر چەمکی ڕات , دەکرێت بڵێین ئەم درێژکراوەیە بۆ هاککەر ناشێت ، چونکە هەرسێ جۆری ڕاتەکان دەگرێتە خۆ ، ئەویش (Remote Access Tool) یاخود (Remote Access Tools)ە.
- هەر لەبواری کۆمپیوتەر و نێت وۆرکدا چەمکێکی تر یاخود درێژکراوەیەکی تری RAT هەیە ئەویش (Remote Access Technology) کەبۆ دەستبەسەراگرتنی پارچە ڕەقەکانی سەر تۆڕێکی ناوخۆیی یان دەرەکی دەبێت و ئەم درێژکراوەیە بەکار دەبرێت لە دام و دەزگا حکومیەکاندا.
- بەرنامەی (Robust Audio Tool) بەهەمان شێوە کورتکراوەکەی RATە ، کەبۆ بواری میدیا و دەنگ بەگشتی بەکاردێت.
- وە دواجار RAT بە جرج یاخود مشکی زۆر گەورە دەگوترێت.

ئەم بابەتە وێنەی فێرکاری بە دوو شێوەی جودا دادەنێم تا لای تۆی خوێنەر بمێنێتەوە ، بە شێوەی pdf و شێوەی jpg وە بەدەر لەوەی ڕاستەوخۆ لەبەردەمت حازرە.

h4kurd.com
by: SchoolsBahareen (SfD)